搜索引擎的魅力

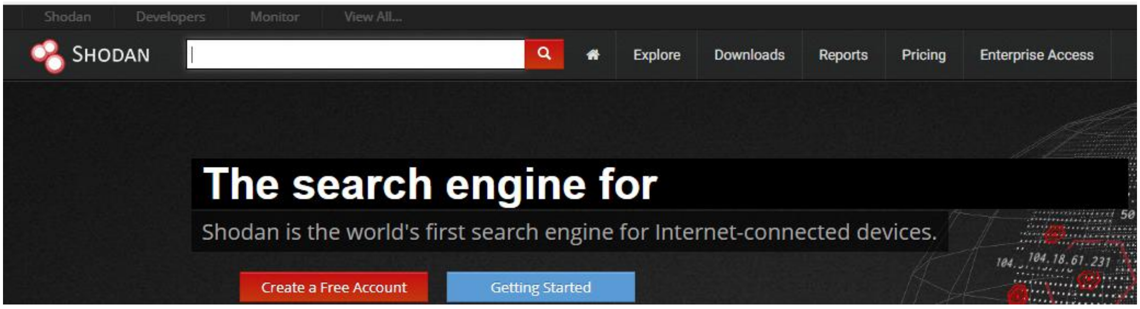
云顶

前言：
大家做这一行相比接触最多的除了浏览器就是搜索引擎，因为往往在你走投无路的时候搜索引擎时常给你带来出其不意的惊喜，如今市面上的搜索引擎五花八门、各式各样反而让很多新手朋友或者一些“老人”迷失了双眼。下面我介绍平时大家用得比较多的几款搜索引擎以及用途方法，如何使你快速的使用它搜索到你想要的东西。

1. Shodan（撒旦）

https://www.shodan.io

shodan 可以进行全球的设备搜索，物联天下，shodan 第一；注册账号才能查看更多,使用更多功能。



http.favicon.hash:icon 批量搜索冒号后面跟每个公司的 icon 值

例如：http.favicon.hash:-1083632446　这是所有带百度 logo 的主机，-1083632446 就是百度的 icon 值

port:搜索端口，例如 port:”22”

org:搜索 ip 所属组织机构，例如 org:”baidu”

OS:搜索操作系统类型，例如 OS:”windows”

http.server:搜索 http 请求返回中 server 的类型，例如 http.server:apache

http.status:搜索 http 请求返回响应码的状态,例如 http.status:200

city:搜索指定城市，例如 city:”beijing”

country: 搜索指定国家，例如 country:“cn”

hostname：搜索指定的主机或域名，例如 hostname:"baidu"

product：搜索指定的操作系统/软件/平台，例如 product:"Apache httpd"

vuln: CVE 漏洞编号，例如：vuln：CVE-2014-0723

net: 搜索一个网段，例如：123.23.1.0/24

几个搜索摄像头的语法：1.Basic realm=” IP Camera” Country:CN 2.JAWS/1.0 2. Camera Country:CN 4.webcam country:cn 5.Webcam Server -Authenticate 6.MikroTIKs-webs 7.IP camera 8.NVR Webserver country:cn 9.Hikvision-webs 10.server GNU rsp/1.0

Shodan 如今摄像头、物联网设备搜索都开始收费了，搜索次数也开始限制了，某些功能已经搜索不到了，且行且珍惜。

2.Zoomeye(钟馗之眼)

https://www.zoomeye.org

Zoomeye 众所周知国内比较比较好的网络空间搜索引擎，相比 shodan 更侧重于 web 层面，指纹识别、web 容器一类的 zoomeye 当之无愧。

app:组件名称，例如 app:apache
ver:组件版本，例如 ver:2.0
OS:操作系统，例如 os:window
Service:服务名称，例如 service:vpn
Cidr:网段，例如 cidr:192.168.1.1/24
Devic:设备名，例如 devic:router
keyword:关键字查询，例如 keyword:technology

指纹搜索：例如 php app:dedecms var:5.7
尝试弱口令：例如 php app：phpadmin
搜索摄像设备：1.DVRDVS-Webs　2.JAWS 等等
Zoomeye 对新手来说还是很好上手的，至于组合语句查询也很简单。
图形界面化的东西用起来还是很简单的，（虽然总结起来我感觉有点智障）不过还是希望大家能在实战中有所用途。（每个账户有指定的查询数量，某些相对敏感的信息需要花钱。）

3.Censys

www.censys.io

也是与 shodan 功能相似的一款搜索引擎
1、查询 CIDR 来枚举系统和服务（注意所枚举的任何额外域名）
2、查询顶级域名来枚举系统和服务（注意所枚举的任何额外的 CIDR 范围）
3、查询单目标系统
4、查询搜索字符串（例如：Apache 等。）
主要网站、证书、ipv4 查询，搜索方式就像用百度一样，提供 6 中 API 接口，喜欢写脚本的自己可以尝试调用来查询。（不知道是网络原因还是其他原因直接查太慢了）

3. FOFA（网络空间资产搜索引擎）

https://fofa.so

国内漏洞查询和资产收集比较好的一款搜索引擎于其他搜索引擎都大同小异，功能差别不是

太大。
高级语法需要用管道符连接如： ‘|| ’ ‘&&’
domain= 搜索根域名带有 xx 的网站。例： domain="baidu.com"
host=从 url 中搜索网站注意搜索要用 host 作为名称。例：host= ".edu.cn"
port= 查找对应 443 端口的资产。例：port=3389
protocol= 搜索制定协议类型(在开启端口扫描的情况下有效)。例：protocol=ssh
cert=搜索证书(https 或者 imaps 等)中带有域名的资产。例：cert=baidu.com
banner= 搜索协议中带有账户文本的资产。例：banner=users && protocol=ftp
type=搜索所有协议资产，支持 subdomain 和 service 两种。例：type=servicce
server== 搜索服务器、中间件名称。例： server=apache
高级语法
title!="powered by" && body=discuz 查询指定 cms 的管理系统
body=”后台”&&domain=”xxx.com” 查询指定域名的后台
Header=”Hikvision” 找摄像头
注意：==符号是完全匹配，加快搜索时间 &&之类的逻辑符都可以用，搜索语法类似 Google

4. PunkSPIDER(全球 web 应用程序漏洞扫描引擎)

www.punkspider.org

全球最大的暗网爬虫、以及漏洞扫描搜索引擎。

Ps：反正就是很牛逼，我也没用过，总结不出来啥。需要了解的自行翻墙查看。

5. IVRE(Drunk)

https://ivre.rocks

一款强大的开源网络侦查工具，严格意义来说不能说是搜索引擎，但它偏偏又是，搞不懂。

Ps：没图片我也没怎么用过，要了解自行百度看文章（上面那段话我也是百度的），要使用最好翻墙。

6. 傻蛋

www.oshadan.com

名符其实的傻蛋浏览器，感觉就是盗版的 shodan，最可耻的是还要收费，对！

就是收费，可以免费使用但是要注册。我嫌麻烦就没有去弄了。

下面的也能百度到：

1 海康威视：超级用户：admin，超级用户密码：12345 关键字:HIkvision

2 大华网络摄像机：用户名：admin，密码：888888 关键字:HDC HF HFW DH

3 天地伟业网络摄像机：用户名：Admin   密码：111111 关键字：JAVWS

总结：

Google 之所以我没提是因为我相信大家肯定都会，而且也真的是很强大的搜索引擎，相比某度不止强一点半星。找到适合自己才是最好的。

大多数搜索引擎都差不多的无非就是调用 nmap、zmap、xmap 等等，谁框架牛逼就是谁厉害。还有搜索引擎和浏览器有本质的区别不要混为一谈。